

Revista Estudos do ISCAA, IIª Série, 5 (1999) 189-212

**POLINÓMIOS E FUNÇÕES POLINOMIAIS
FACTORIZAÇÃO NO ANEL DOS POLINÓMIOS**

MARGARIDA MARIA SOLTEIRO MARTINS PINHEIRO

*PROFESSORA ADJUNTA DE MATEMÁTICA
DO ISCAA*

RESUMO:

O presente artigo faz parte de um dos temas discutidos no concurso de provas públicas para professores-adjuntos do ensino superior politécnico realizado em Dezembro de 1994. Após a introdução de alguns conceitos básicos, passa-se ao estudo da irredutibilidade de um polinómio, do ponto de vista dos corpos dos números complexos, reais e irracionais.

Palavras-Chave

Anel de polinómios, grau de um polinómio; função polinomial; raiz de um polinómio; factorização de um polinómio; polinómio irredutível.

PRELIMINARES

O que é um polinómio?

Em cursos elementares de álgebra definimos muitas vezes polinómio como uma expressão da forma $x^3 - \frac{1}{2}x^2$ ou, mais genericamente, $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ em que os a_i são chamados coeficientes e são usualmente números reais. Por esta definição, x é um polinómio.

Mas o que é “ x ”?

A resposta mais vulgar é a de que “ x ” é uma incógnita; isto é, um número pertencente ao mesmo conjunto dos coeficientes mas que não está especificado.

Outra resposta à questão “O que é x ?” é dada, pondo em destaque que o que realmente tem significado é uma função f , cujo valor em x é dado, por exemplo, por $f(x) = x^3 - \frac{1}{2}x^2$. Neste sentido “ x ” é afinal o nome genérico de um elemento do domínio da função. A esta função chamamos função polinomial, definida sobre um corpo e que toma valores nesse corpo. (Por exemplo, funções reais de variável real). Através desta perspectiva podemos até dar uma definição recursiva de função polinomial:

Seja K um anel comutativo.

Chamamos funções polinomiais a todas funções $f: K \rightarrow K$ tais que

i) Para cada $k \in K$ a função constante $f(x) = k$ com $x \in K$ é uma função polinomial;

ii) A função identidade $f(x) = x$ para todo o $x \in K$, é uma função polinomial;

iii) Se $f(x)$ e $g(x)$ são funções polinomiais, então também são funções polinomiais $(f + g)(x) = f(x) + g(x)$ e $(f \cdot g)(x) = f(x) \cdot g(x)$

Observe-se que esta definição inclui tão somente as funções do tipo $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$.

Mas às vezes dois polinômios distintos induzem a mesma função, logo esta correspondência não seria sequer aplicação. Por exemplo, x e x^2 são dois polinômios distintos que dão origem à mesma função em Z .

Outra resposta à questão “O que é x ?” pode ser a de que é um símbolo. E o que representa?

A abordagem que vamos aqui seguir, começa por definir polinômio para finalmente chegar à definição de função polinomial, pretendendo que a resposta à questão anterior seja pelo menos não tão embaraçosa.

ANÉIS DE POLINÓMIOS

Definição 1

Seja $(A, +, \cdot)$ um anel. Chamamos polinômio f sobre A , a toda a sequência do tipo $\{(a_0, a_1, \dots, a_n, \dots): a_i \in A\}$ onde apenas um número finito de termos é não nulo. Como consequência, verifica-se que, para cada polinômio não nulo f , existe um inteiro não negativo n tal que $a_n \neq 0$ com $a_j = 0, \forall j > n$. Ao número inteiro n chamamos grau do polinômio f , que representamos por $gr(f)=n$ e a a_n chamamos coeficiente principal de f .

(Por questões de notação e de agora em diante, sempre que não haja perigo de confusão, representaremos o anel $(A, +, \cdot)$ simplesmente por A)¹

Definição 2

No conjunto de todas as sequências $\{(a_0, a_1, \dots, a_n, \dots): a_i \in A\}$ definimos duas operações, a saber:

$$(a_0, a_1, \dots) \oplus (b_0, b_1, \dots) = (a_0 + b_0, a_1 + b_1, \dots)$$

$$(a_0, a_1, \dots) \otimes (b_0, b_1, \dots) = (c_0, c_1, \dots) \text{ onde}$$

$$c_0 = a_0 b_0$$

¹ Como caso particular, refira-se que o grau do polinômio nulo não está definido.

$$c_1 = a_0 b_1 + a_1 b_0$$

$$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$$

...

$$c_r = \sum_{i+j=r} a_i b_j$$

Teorema 1

Seja A um anel. Então o conjunto dos polinómios sobre A , munido das operações \oplus e \otimes atrás definidas, ainda é um anel, a que chamamos anel de polinómios.

Demonstração:

A verificação de que a adição de polinómios forma um grupo abeliano, resulta imediatamente da própria definição da operação \oplus feita termo a termo sobre as sequências e do facto de A ser grupo abeliano. O zero do anel é a sequência do tipo $(0, 0, \dots, 0, \dots)$ e a que chamamos polinómio nulo.

Para provar a associatividade da operação \otimes , teremos de provar que $f \otimes (g \otimes h) = (f \otimes g) \otimes h$ onde f, g, h são polinómios sobre A . Para a demonstração calculemos o r -ésimo termo de cada membro. Sejam $f = (a_0, a_1, \dots)$, $g = (b_0, b_1, \dots)$ e $h = (c_0, c_1, \dots)$. O p -ésimo termo de $(g \otimes h)$ é dado por $\sum_{i+j=p} b_i c_j$. Donde, o r -ésimo termo de $f \otimes (g \otimes h)$

vem

$$\sum_{q+p=r} a_q r_p = \sum_{p+q=r} a_q \left(\sum_{i+j=p} b_i c_j \right) = \sum_{i+j+q=r} a_q (b_i c_j)$$

Analogamente, o r -ésimo termo de $(f \otimes g) \otimes h$ vem

$$\sum_{l+j=r} s_l c_j = \sum_{l+j=r} \left(\sum_{q+i=l} a_q b_i \right) c_j = \sum_{q+i+j=r} (a_q b_i) c_j$$

Para provar a distributividade da operação \otimes relativamente à operação \oplus , temos de provar que $f \otimes (g \oplus h) = (f \otimes g) \oplus (f \otimes h)$. Calculando os termos de ordem r de cada membro, encontramos

$$\sum_{i+j=r} a_i (b_j + c_j) \text{ e } \sum_{i+j=r} a_i b_j + \sum_{i+j=r} a_i c_j \text{ respectivamente.}$$

Pela distributividade em A tiramos a conclusão pretendida. ♣

De modo a que a abordagem adoptada se aproxime da visão usual dos polinómios, introduzimos de seguida algumas notações. Designemos por ax^r o polinómio $(0,0,\dots,a,0,\dots)$ onde a é o $(r+1)$ -ésimo termo do polinómio. Assim, por exemplo, $ax^0=(a,0,\dots)$ e $ax^1=(0,a,0,\dots)$.

Então, se f é um polinómio de grau n $(a_0, a_1, \dots, a_n, 0, \dots)$ pode tomar a forma $a_0x^0 + a_1x^1 + \dots + a_nx^n$. Simplificando a escrita e representando simplesmente por a o polinómio ax^0 e por ax o polinómio ax^1 verificamos então que qualquer polinómio $(a_0, a_1, \dots, a_n, 0, \dots)$ pode ser escrito como $a_0 + a_1x + \dots + a_nx^n$; é esta convenção que estabelece a ligação entre a definição 1 e a definição de polinómio que já conhecíamos.

Designemos a partir de agora e pelas razões apontadas, por $A[x]$ o anel dos polinómios sobre A na indeterminada x . Os elementos de $A[x]$ são geralmente representados por letras minúsculas, por exemplo f ou mais geralmente por $f(x)$. Aos elementos de A identificados com $A[x]$ chamamos polinómios constantes.²

Outra forma de relacionar as duas definições dadas tem por base o seguinte teorema:

² Repare-se que a definição agora dada de polinómio é coerente com a definição usual de polinómio. Assim, dados os polinómios $p_1(x) = x^2 - 3x + 2$ e $p_2(x) = x^5 + 4x^3 - 3x^2 + 1$ a sua soma é o polinómio $p_3(x) = x^5 + 4x^3 - 2x^2 + 3x - 1$. Utilizando a definição 1, temos $p_1=(2,-3,1,0,0,\dots)$ $p_2=(1,0,-3,4,0,1,0,0,\dots)$ e $p_1+p_2=(3,-3,-2,4,0,1,0,0,\dots)$ que representa p_3 na nova notação.

Teorema 2

Seja:

$$\varphi: A \rightarrow A[x]$$

$$r \rightarrow (r, 0, \dots). \text{ Então } \varphi \text{ é um monomorfismo.}$$

Demonstração:

Queremos provar que $\varphi(r+s) = \varphi(r) \oplus \varphi(s)$ e ainda que $\varphi(rs) = \varphi(r) \otimes \varphi(s)$ para todos os elementos r, s de A . Ora, por construção $\varphi(r+s) = (r+s, 0, 0, \dots)$ e pela definição 2 $\varphi(r) \oplus \varphi(s) = (r, 0, \dots) \oplus (s, 0, \dots) = (r+s, 0, \dots)$.

De modo análogo provaríamos a segunda relação. ♣

Como consequência do teorema $\varphi(A) = \{(r, 0, \dots) \mid r \in A\}$ é um subanel de $A[x]$ isomorfo a A , o que justifica a equivalência das duas definições.

No que se segue, utilizaremos pois a notação $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ em vez da notação indicada na definição 1, tendo sempre em conta que um polinómio pode ser encarado como uma sequência de coeficientes³.

GRAU DE UM POLINÓMIO

Recorde-se que ao introduzirmos na definição 1 a noção de grau de um polinómio, associamos a cada polinómio não nulo, um número inteiro não negativo. Por convenção tome-se $\text{gr}(0) = -\infty$.

Onde 0 representa o polinómio nulo. Temos assim:

$$\text{gr} : A[X] \rightarrow \mathbb{Z}_0^+ \cup \{-\infty\}$$

$$f \rightarrow \text{gr}(f) = n$$

³ A partir de agora e caso não haja dúvidas, representaremos apenas por + e x as operações definidas na definição 2.

Ainda por convenção $(-\infty)+(-\infty)=(-\infty)$ com $(-\infty)<n$, sendo n um número inteiro não negativo.

Proposição 1

Sejam $f, g \in A[x]$. Então $gr(f + g) \leq \max\{gr(f), gr(g)\}$ e $gr(fxg) \leq gr(f) + gr(g)$

Teorema 3

Se A é um domínio de integridade então $A[x]$ é um domínio de integridade e nestas condições $gr(fxg) = gr(f) + gr(g) \forall f, g \in A[x]$

Demonstração:

No teorema 1 foi já demonstrado que, sendo A um anel, também $A[x]$ é um anel. Por outro lado, é imediato que, se A é um anel comutativo com elemento unidade, também $A[x]$ é um anel comutativo cujo elemento unidade é o polinómio constante 1 (distinto do polinómio nulo). Falta provar que, se A não tem divisores de zero também $A[x]$ não tem.

Para tal, considerem-se dois elementos f e g de $A[x]$, não nulos, tais que

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \text{ com } a_n \neq 0$$

$$\text{e } g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0 \text{ com } b_m \neq 0$$

Então, por definição, $(fxg)(x) = c_{n+m} x^{n+m} + \dots + c_1 x + c_0$ onde os c_i se determinam de acordo com a definição 2. Como A é domínio de integridade e $a_n \neq 0$ e $b_m \neq 0$, tem-se $a_n b_m \neq 0$. Mas $a_n b_m = c_{m+n}$.

Logo $fxg \neq 0$. Provámos assim que, sendo f e g dois elementos não nulos de $A[x]$ se tem $fxg \neq 0$ o que prova não existirem divisores de zero em $A[x]$. Conjugando este resultado com as conclusões anteriores, fica provado que $A[x]$ é um domínio de integridade.

Do que foi dito podemos também concluir que $gr(fxg) = n + m = gr(f) + gr(g) \forall f, g \in A[x]$ c.q.d. ♣

FUNÇÕES POLIMONIAIS

Definição 3

Seja A um anel. Uma função $\psi: A \rightarrow A$ diz-se uma função polinomial se existe um polinómio $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ de $A[x]$ tal que, para todo o $b \in A$ se tem $\psi(b) = a_n b^n + a_{n-1} b^{n-1} + \dots + b_1 x + b_0$.⁴

POLINÓMIOS SOBRE UM CORPO

Iremos falar de seguida de polinómios sobre um corpo, dado que, de um certo modo, podemos dizer que o anel $A[x]$ é particularmente “bem comportado” quando A é um corpo.

Teorema 4

Seja K um corpo e sejam $f, g \in K[x]$ dois polinómios. Sendo $g \neq 0$ existem $q, r \in K[x]$ tais que $f = gq + r$ onde $gr(r) < gr(g)$ ou $r = 0$. Os polinómios q e r assim definidos são únicos.

Demonstração:

1ª parte: demonstração da existência dos polinómios q e r .

É claro que, se $f = 0$ então o teorema verifica-se trivialmente com $q = r = 0$. Suponhamos $f \neq 0$ e seja $gr(f) = n$ e $gr(g) = m$. Note-se que, se $n < m$ então basta fazer $q = 0$ e $r = f$. Consideremos então $n \geq m$. Vamos proceder por indução sobre n . Se $gr(f) = 0$, isto é, se $n = 0$, vem $gr(g) = 0$ pelo que os polinómios são constantes. Nesse caso a existência de q e r está garantida, uma vez que K é corpo. (Recorde-se que, num corpo,

⁴ Cada polinómio $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ pode obviamente ser associado à função definida em A cujo valor em $b \in A$ é dado por $a_n b^n + a_{n-1} b^{n-1} + \dots + b_1 x + b_0$ e que notaremos por

$f(b) = a_n b^n + a_{n-1} b^{n-1} + \dots + a_1 b + b_0$.

as equações do tipo $ax=b$ têm uma única solução do tipo $a^{-1}b$). De facto, sendo $f=a$ e $g=b$, com $a,b \in K$ e $b \neq 0$, basta fazer $r=0$ e $q=ab^{-1}$. Admita-se agora a veracidade da proposição para todo o f tal que $gr(f) < n$. Sejam $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ com $a_n \neq 0$ e $g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$ com $b_m \neq 0$

Consideremos o polinómio $q_1 = a_n b_m^{-1} x^{n-m}$. Obtem-se assim:

$$f = gq_1 + r_1 \quad (1)$$

com $r_1 = f - gq_1$ onde $gr(r_1) < n$ ou $r_1 = 0$.

Pretendemos provar que a proposição ainda é válida para $gr(f) = n$.

Ora, sendo ainda $r_1 \in K[x]$, e por hipótese de indução, existem polinómios q_2 e r_2 de $K[x]$, tais que $r_1 = gq_2 + r_2$ com $r_2 = 0$ ou $gr(r_2) < gr(g)$. Substituindo em (1) vem $f = gq_1 + gq_2 + r_2$ ou seja $f = g(q_1 + q_2) + r_2$. Fazendo $q = q_1 + q_2$ e $r = r_2$ tem-se finalmente $gr(r) < gr(g)$ ou $r = 0$, o que dá por findo o processo de indução e demonstra a existência de q e r .

2ª parte: demonstração da unicidade de q e r

Por absurdo, suponhamos que q e r não eram únicos; isto é,

$$f = gq + r \text{ com } r = 0 \text{ ou } gr(r) < gr(g)$$

$$f = gq' + r' \text{ com } r' = 0 \text{ ou } gr(r') < gr(g) \text{ (com } q \neq q' \text{ ou } r \neq r').$$

Mas então $gq + r = gq' + r'$. Pelas propriedades do corpo $g(q - q') = r' - r$. Pelo Teorema 3,

$$gr(g(q - q')) = gr(g) + gr(q - q'). \text{ Logo } gr(g) + gr(q - q') = gr(r' - r).$$

Por outro lado, pela proposição 1, $gr(r' - r) \leq \max\{gr(r'), gr(r)\}$.

Mas, por hipótese, $\max\{gr(r'), gr(r)\} < gr(g)$.

Logo $gr(g) + gr(q - q') < gr(g)$; ou seja $gr(q - q') < 0$. Mas então $gr(q - q') = -\infty$; atendendo às convenções feitas resulta $q - q' = 0$ e portanto $q = q'$. Onde resulta, $f = gq + r$ e $f = gq + r'$ e finalmente $r = r'$, como pretendido. ♣

POLINÓMIOS DE VÁRIAS VARIÁVEIS

Antes de continuarmos o nosso estudo sobre polinómios e sua factorização, façamos referência, ainda que breve, a polinómios de várias variáveis.

Consideremos o polinómio $x^2 + xy + y^2$. Podemos considerá-lo como um polinómio em y com coeficientes em $A[X]$. Tal afirmação tem sentido, bastando fazer $B = A[X]$ que é um anel, tal que $B[Y] = A[X, Y]$.

Se agora considerássemos o polinómio $z^2x + 2(x+y)z$, podíamos, de um modo idêntico, pensá-lo como um polinómio em z com coeficientes em $A[X, Y]$ e que notaremos por $A[X, Y, Z]$. A definição é indutiva.

Definição 4

Seja A um domínio de integridade e seja $A^{(0)} = A$. Define-se indutivamente $A^{(n)}$ tal que $A^{(n)} = A^{(n-1)}[X]$.

De outro modo, se $f \in A^{(n)}$ então f pode ser escrito como uma sequência (a_0, a_1, \dots) com $a_i \in A^{(n-1)}$. (Isto é, cada a_i é ainda uma outra sequência e assim sucessivamente).

RAIZ DE UM POLINÓMIO. TEOREMA DA FACTURIZAÇÃO.

Definição 5

Seja $f \in A[X]$ onde A é um domínio de integridade. Chama-se raiz de f a todo o elemento $c \in A$ tal que $f(c) = 0$.

Apresentamos de seguida um teorema que caracteriza as raízes de um polinómio de $K[X]$, sendo K um corpo.

Teorema 5 (Teorema da factorização)

Seja K um corpo e $f \in K[X]$. Então $a \in K$ é uma raiz de f se e só se $x-a$ é um divisor de f .

Demonstração:

(\Rightarrow)

Suponhamos que a é raiz de f . Consideremos um polinómio $x-a$. Pelo teorema 4, sabemos que existem polinómios $q, r \in K[X]$ tais que $f = (x-a)q + r$ com $r=0$ ou $\text{gr}(r) < 1$. Ou seja, $r=0$ ou r é uma constante. Em particular e para $x=a$, tem-se $f(a) = (a-a)q(a) + r$ e logo $f(a) = r$.

Como, por hipótese a é raiz de f , resulta $r = f(a) = 0$. Concluimos assim que o resto da divisão de f por $x-a$ é igual a zero; ou seja, f é divisível por $x-a$.

(\Leftarrow)

Para provar a implicação em sentido contrário, comecemos por admitir que $x-a$ é um divisor de f . Isto é, que existe $q \in K[X]$ tal que $f = (x-a)q$. Em particular, $f(a) = (a-a)q$ donde resulta $f(a) = 0$. Mas tal significa que a é raiz de f , como queríamos provar. ♣

Definição 6

A raiz a de um polinómio f diz-se de multiplicidade k se $(x-a)^k$ é um divisor de f mas $(x-a)^{k+1}$ já não é divisor de f .

Teorema 6

Seja $f \in K[X]$ e $a \in K$.

a é uma raiz de f de ordem de multiplicidade r se e só se $f = (x-a)^r q$ onde $q \in K[X]$ e tal que a não é raiz de q .

Demonstração:

(\Rightarrow)

Ora, por definição, sendo a uma raiz de f de ordem de multiplicidade r , sabemos que $(x-a)^r$ é um divisor de f . Em particular $f = (x-a)^r q$ para algum $q \in K[X]$. Queremos provar que a não é raiz de

q . Por absurdo e se tal acontecesse então q era divível por $x-a$ e poderíamos escrever $q=(x-a)q'$ para algum $q' \in K[X]$. Mas então $r=(x-a)^{r+1}q'$ e $(x-a)^{r+1}$ dividiria f o que contradiz a definição de a ser raiz de ordem de multiplicidade r . O absurdo resultou de se ter suposto que a era raiz de q . Logo, concluímos que a não é raiz de q , como pretendíamos.

(\Leftarrow)

Para provar a implicação contrária, consideremos $f=(x-a)^r q$, com $q \in K[X]$. Por absurdo, suponhamos que a é uma raiz de f de ordem de multiplicidade m , com $m > r$. Por definição $f=(x-a)^m q_1$, para algum $q_1 \in K[X]$. Mas então e pela transitividade, $(x-a)^r q=(x-a)^m q_1$; donde $(x-a)^{m-r} q_1=q$, com $m-r > 0$, o que significa que a é raiz de q , o que contraria a hipótese. O absurdo resultou de se ter suposto que a era raiz de f de ordem superior a r . Logo podemos concluir que a é raiz de f de ordem de multiplicidade r , como pretendíamos. ♣

Outro teorema essencial da teoria de aneis de polinómios diz respeito ao número de raízes de um polinómio.

Teorema 7

Seja K um corpo e $f \in K[X]$. Se $gr(f)=n$, com $n > 0$, então f tem no máximo, n raízes distintas em K .

Demonstração:

Vamos proceder por indução sobre n .

Se $gr(f)=1$ então tem-se $f=a_0+a_1x$ e $-a_0a_1^{-1}$ é a única raiz de f . Logo a proposição é verdadeira para $n=1$. Admita-se a proposição verdadeira para $n-1$; isto é, que se um polinómio tem grau $n-1$, então tem, no máximo, $n-1$ raízes distintas.

Seja f tal que $gr(f)=n$. (É claro que se f não tem nenhuma raiz, o teorema fica imediatamente demonstrado). Suponhamos então que f admite pelo menos uma raiz, seja a . Pelo teorema da factorização,

existe $q \in K[X]$ tal que $f = (x-a)q$. Pelo teorema 3 e atendendo a que todo o corpo é domínio de integridade, podemos escrever $gr(f) = gr(x-a) + gr(q)$; ou seja, $n = 1 + gr(q)$. Logo $gr(q) = n-1$. Por hipótese de indução, q tem no máximo $n-1$ raízes distintas. Mas, porque $f = (x-a)q$ qualquer raiz de f , distinta de a , é também raiz de q , pelo que se pode concluir que f tem, no máximo, n raízes distintas. c.q.d. ♣

Antes da definição propriamente dita de polinómios irredutíveis, vamos introduzir novos conceitos.

Definição 7

Seja A um anel comutativo com elemento identidade 1 . Um elemento e de A diz-se uma unidade se $c.e = 1 = e.c$, para algum c de A . Designamos por $U(A)$ o conjunto de todas as unidades de A .

Definição 8

Seja A um anel comutativo com elemento identidade 1 e seja b um elemento de A . Um elemento a de A diz-se um associado a b se e só se $a = be$, onde e é uma unidade.

Definição 9

Seja A um domínio de integridade. Um elemento r de A diz-se irredutível se :

- i) $r \notin U(A)$
- ii) Se $r = ab$, então ou a é uma unidade ou b é uma unidade.

Definição 10

Um domínio de integridade A diz-se um domínio de factorização única (DFU) se:

- i) Todo o elemento $a \in A \setminus \{0\}$ admite uma factorização do tipo $a = u.a_1.a_2....a_n$ onde $u \in U(A)$, $n \geq 0$ e a_i é irredutível, para $i = 1, ..., n$.

ii) Tal factorização é única; isto é, se $u.a_1.a_2....a_n = u'.a'_1.a'_2....a'_m$ com $u, u' \in U(A)$, $n \geq 0$, $m \geq 0$, a_i, a_j irredutíveis, para $i=1,...,n$ e $j=1,...,m$ então $n=m$ e existe uma permutação π de $\{1,2,...,n\}$ tal que a_i é associado de $a'_{\pi(i)}$.

Definição 11

Seja A um domínio de integridade e v uma função tal que $v: A \rightarrow Z_0^+$ e que verifica as condições:

- a) $\forall a \in A, \forall b \in A \setminus \{0\}, \exists q, r \in A: a = bq + r$ com $r=0$ ou $v(r) < v(b)$
- b) $\forall a, b \in A \setminus \{0\}, v(a) \leq v(b)$

À estrutura formada pelo domínio de integridade A munido da função v assim definida chamamos domínio eucladiano.

Como consequência desta definição e do que até aqui foi visto, podemos concluir que “Se K é corpo, então $K[X]$ munido da função grau, é um domínio eucladiano”

Definição 12

Seja K um corpo e $p \in K[X]$. Diz-se que p é um polinómio irredutível sse:

- i) p não é um polinómio constante;
- ii) Para todos os $g, h \in K[X]$ se $p=gh$, então ou h é um polinómio constante não nulo ou g é um polinómio constante não nulo.

A questão seguinte é a de saber quais são os polinómios irredutíveis em $K[X]$. Antes porém verifiquemos que:

Proposição 2

Se $p \in K[X]$ é um polinómio de grau um, então p é irredutível.

Demonstração:

De facto, se p é um polinómio de grau um, então p não é constante. Falta provar que, se $p=gh$ com $g,h \in K[X]$, então g é um polinómio constante não nulo ou h é um polinómio constante não nulo. Suponhamos, por exemplo, que g não é um polinómio constante. Logo $gr(g) \geq 1$. Por absurdo, suponhamos que h também não é um polinómio constante e logo $gr(h) \geq 1$. Pelo teorema 3 $gr(p)=gr(g)+gr(h)$. Logo $gr(p) \geq 2$ o que contradiz a hipótese. O absurdo resultou de se ter suposto que h não era constante. Logo h é um polinómio constante. c.q.d. ♣

Proposição 3

Seja $u \in U(A)$ e $v \in A$ tal que $u=k v$ para algum $k \in A$. Então $v \in U(A)$.

Demonstração:

Queremos provar que existe $v' \in A$ tal que $v.v'=1=v'.v$. Ora, por hipótese, $\exists u' \in A: u.u'=1=u'.u$. Substituindo atrás, vem $1=u.u'=(kv).u'=(u'k).v$; pelo que basta tomar $v'=u'k$.

De modo análogo procederíamos para a outra igualdade. ♣

Iremos de seguida abordar a questão dos polinómios irredutíveis nos casos de $C[X], R[X], Q[X]$.

POLINÓMIOS IRREDUTÍVEIS $C[X]$

O teorema básico que permite determinar os polinómios irredutíveis em $C[X]$ é conhecido pelo teorema fundamental da álgebra.

Teorema 8 (Teorema fundamental da Álgebra)

Todo o polinómio $p \in C[X]$ de grau superior ou igual a um, tem uma raiz em C .

Para a demonstração, ver “A concrete introduction to higher algebra” de Lindsay Childs; 1979, Springer Verlag.

Como consequência apresentamos o corolário seguinte:

Corolário

$p \in C[X]$ é um polinómio irredutível se e só se $gr(p)=1$
(Isto é, em C os únicos polinómios irredutíveis são do primeiro grau).

Demonstração:

Já vimos que se o grau de p é um, então p é irredutível. Falta provar a implicação contrária; suponhamos que $p \in C[X]$ é um polinómio irredutível. Então $gr(p) \geq 1$. Logo, pelo teorema fundamental da álgebra, p tem uma raiz em C . Designemos por α tal raiz. Por outro lado e atendendo ao teorema 5, $p=(x-\alpha)q$, par algum $q \in C[X]$. Ora, como p é irredutível e $(x-\alpha) \notin U(C[X])$ resulta, pela proposição 3 que $q \in U(C[X])$. Mas então q é um polinómio constante não nulo e logo $gr(p)=1$. c.q.d. ♣

POLINÓMIOS IRREDUTÍVEIS $R[X]$

Analisemos o estudo da irredutabilidade de polinómios com coeficientes em R à luz do resultado seguinte.

Teorema 9

$p \in R[X]$ é um polinómio irredutível se e só se $gr(p)=1$ ou $p=ax^2+bx+c$ com $a \neq 0$ e $b^2 - 4ac < 0$

(Isto é, os polinómios irreduzíveis em $R[X]$ são os de primeiro grau e todos os de segundo grau cujo binómio discriminante é negativo).

Demonstração:

(\Rightarrow)

Seja $p \in R[X]$ um polinómio irreduzível. Então $gr(p) \geq 1$. Se $gr(p)=1$ o teorema fica provado. Caso contrário, suponha-se $gr(p) \geq 2$. Pelo teorema 8 e porque $R \subset C$, p tem pelo menos uma raiz complexa. Seja α tal raiz. Então podemos escrever $\alpha = w + si$ com $s \neq 0$. Seja $h = (x - \alpha)(x - \bar{\alpha})$ com $\bar{\alpha} = w - si$. Efectuando os cálculos facilmente se verifica que então $h \in R[X] \setminus \{0\}$. Então e pelo teorema 4, existem $q, r \in R[X]$ tais que $p = hq + r$ com $r=0$ ou $gr(r) < gr(h)$ sendo $gr(h)=2$. Suponhamos $gr(r) < 2$; isto é, $r = a_1x + a_0$ com $a_0, a_1 \in R$. Por outro lado e como α é raiz de p tem-se $p(\alpha)=0$. Portanto $0 = p(\alpha) = (hq+r)(\alpha) = h(\alpha)q(\alpha) + r(\alpha) = r(\alpha)$.

Isto é, $r(\alpha)=0$

ou seja $a_1(\alpha) + a_0 = 0$

$a_1(w+si) + a_0 = 0$

$(a_0 + a_1w) + a_1si = 0$

Donde resulta $(a_0 + a_1w) = 0$ e $a_1s = 0$. Como $s \neq 0$ resulta $a_1 = 0$ e portanto $a_0 = 0$. Mas então $r=0$ donde $p=hq$, com $h \in R[X] \setminus \{0\}$, $q \in R[X]$ e $gr(h)=2$. Como, por hipótese p é irreduzível, tem-se que q é um polinómio constante não nulo, donde $gr(h) = gr(p) + gr(q) = 2 + 0 = 2$.

Seja $p = ax^2 + bx + c$. Como sabemos este polinómio tem duas raízes, $\alpha_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}$ e $\alpha_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a}$, que só são

reais se $b^2 - 4ac \geq 0$. Mas, se tais raízes fossem iguais, o polinómio p poderia ser escrito $p = a(x - \alpha_1)(x - \alpha_2)$, com a constante, o que contraria a hipótese de $p \in R[X]$ ser um polinómio irreduzível. Logo $b^2 - 4ac < 0$.

(\Leftarrow)

Já vimos que, se $gr(p)=1$ então p é irredutível. Suponha-se então $p=ax^2+bx+c$ com $a \neq 0$ e $b^2 - 4ac < 0$. Logo p não é uma unidade. Sejam $f, g \in R[X]$ tais que $p=fg$; e $gr(p)=2$. Ou seja, $gr(f)+gr(g)=2$. Portanto, ou $gr(f)=2$ e $gr(g)=0$ ou $gr(f)=1$ e $gr(g)=1$ ou $gr(f)=0$ e $gr(g)=2$. Mas, se fosse $gr(f)=gr(g)=1$ e sendo $p=fg$, resultava que p tinha duas raízes reais o que contradiz o facto de $b^2 - 4ac < 0$. Concluimos então que

$$p = fg \Rightarrow (gr(f) = 2 \wedge gr(g) = 0) \vee (gr(f) = 0 \wedge gr(g) = 2).$$

Ou seja, $p = fg \Rightarrow g \in U(R[X]) \vee f \in U(R[X])$.

Resumindo, provámos que:

i) $p \notin U(R[X])$

ii) $\forall f, g \in R[X] \quad p = fg \Rightarrow f$ é um polinómio constante não nulo ou g é um polinómio constante não nulo; c.q.d. ♣

POLINÓMIOS IRREDUTÍVEIS $Q[X]$

Vimos anteriormente como resolver o problema da determinação de polinómios irredutíveis em $C[X]$ e em $R[X]$. Vejamos o que se passa em $Q[X]$. Ora, até hoje, ninguém conhece uma resposta para a questão “Quais os polinómios irredutíveis em $Q[X]$?” O que se conhece são apenas condições suficientes. Assim, sendo $f \in Q[X]$ basta multiplicar o polinómio f por um inteiro suficientemente grande para que todos os coeficientes resultem inteiros. O polinómio assim encontrado tem exactamente as mesmas raízes que o polinómio dado. Ou seja, se conseguirmos factorizar o polinómio inicial com coeficientes em Q , também conseguimos factorizar o polinómio encontrado com coeficientes inteiros e queremos é saber se esta factorização é ou não irredutível sobre os racionais. Seja

$$p = a_0 + a_1x + \dots + a_nx^n \in Q[X] \text{ onde, para cada } i=0, \dots, n \quad a_i = \frac{p_i}{q_i} \text{ com}$$

$p_i \in \mathbb{Z}, q_i \in \mathbb{Z} \setminus \{0\}, m.d.c.(p_i, q_i) = 1$. Seja ainda $t = m.m.c.(q_0, \dots, q_n)$. Então $t \neq 0$ e podemos escrever p tal que $p = 1/t(tp)$ com $tp \in \mathbb{Z}[X]$. Ora p é irredutível em $\mathbb{Q}[X]$ se e só se tp também é irredutível em $\mathbb{Z}[X]$. Para polinómios em $\mathbb{Z}[X]$ podemos enunciar:

Teorema 10

$p \in \mathbb{Z}[X]$ é irredutível em $\mathbb{Q}[X]$ se e só se p é irredutível em $\mathbb{Z}[X]$.

Para a demonstração, ver “Lectures in abstract algebra I” de Nathan Jacobson; 1975, Springer Verlag.

Deste teorema podemos concluir que a determinação de polinómios irredutíveis em $\mathbb{Q}[X]$ pode reduzir-se à determinação de polinómios irredutíveis em $\mathbb{Z}[X]$.

O teorema seguinte é um critério que permite, sob algumas condições, determinar polinómios irredutíveis em $\mathbb{Z}[X]$.

Teorema 11 (Critério de Eisenstein)⁵

Seja $p = a_0 + a_1x + \dots + a_nx^n$ com $a_n \neq 0$ e $n \geq 2$ um polinómio de $\mathbb{Z}[X]$. Se existe um número primo $\alpha \in \mathbb{Z}$ tal que:

- i) $\alpha \nmid a_n$
- ii) $\alpha \mid a_i$ com $i=0, \dots, n-1$
- iii) $\alpha^2 \nmid a_0$

então p é irredutível em $\mathbb{Z}[X]$.

Antes da demonstração vejamos alguns conceitos preparatórios do teorema enunciado.

⁵ O símbolo \nmid deve ler-se “divide”.

O símbolo \nmid deve ler-se “não divide”.

Definição 13

Seja D um domínio de integridade e r e s elementos de D . Diz-se que r divide s (simbolicamente $r \mid s$) se existe $k \in D$ tal que $s = kr$.

Definição 14

Seja D um domínio de integridade e r um elemento de D . Diz-se que r é um elemento primo em D se e só se:

- i) $r \neq 0$ e $r \notin U(D)$
- ii) Dados $a, b \in D$, se $r \mid ab$ então $r \mid a$ ou $r \mid b$

Posto isto, passemos à demonstração do teorema anterior.

Demonstração (do critério de Eisenstein):

Por absurdo, suponhamos que p não é irredutível em $Z[X]$. Então existem polinômios não constantes, f e g de $Z[X]$ tais que $p = fg$. Suponhamos $f = b_0 + b_1x + \dots + b_rx^r, b_r \neq 0, r \geq 1$ e $g = c_0 + c_1x + \dots + c_sx^s, c_s \neq 0, s \geq 1$ e ainda, sem perda de generalidade que $r \geq s$. Observe-se que e como consequência do teorema 3, $gr(p) = gr(f) + gr(g)$ o que implica $n = r + s$. Da própria construção, resulta

$$a_0 = b_0c_0$$

$$a_1 = b_0c_1 + b_1c_0$$

...

$$a_s = b_0c_s + b_1c_{s-1} + \dots + b_sc_0$$

...

$$a_r = b_0c_r + b_1c_{r-1} + \dots + b_rc_0$$

...

$$a_n = b_rc_s$$

Por hipótese ii) $\alpha \mid a_0$ isto é, $\alpha \mid b_0c_0$. Como α é primo, $\alpha \mid b_0$ ou $\alpha \mid c_0$. Podem então ocorrer três situações:

- 1) $\alpha \mid b_0$ e $\alpha \mid c_0$
- 2) $\alpha \mid b_0$ e $\alpha \nmid c_0$

3) $\alpha \nmid b_0$ e $\alpha \nmid c_0$

Se ocorresse o primeiro caso, tínhamos $b_0 = k\alpha$ e $c_0 = k'\alpha$ com $k, k' \in \mathbb{Z}$. Logo $a_0 = b_0 c_0 = k\alpha k'\alpha = kk'\alpha^2$. Mas então $\alpha^2 \mid a_0$ o que contradiz a hipótese iii). Não podendo ocorrer a situação 1 é porque se deve verificar a situação 2 ou a situação 3. Suponhamos que se verifica a situação 2. Então $\alpha \mid b_0$ e $\alpha \nmid a_1$ e $a_1 = b_0 c_1 + b_1 c_0$ o que implica $\alpha \mid b_1 c_0$. Mas como $\alpha \nmid c_0$ e α é primo, terá de se concluir que $\alpha \mid b_1$. Analogamente $\alpha \mid b_0$ e $\alpha \mid b_1$ e $\alpha \nmid a_2$ e $a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0$ o que implica $\alpha \mid b_2 c_0$. Mas como $\alpha \nmid c_0$ e α é primo, terá de se concluir que $\alpha \mid b_2$. Continuando um raciocínio análogo, concluimos que $\alpha \mid b_j$ com $j=0, \dots, r$. Por último e atendendo a que $a_n = b_r c_s$ e $\alpha \nmid b_r$ conclui-se que $\alpha \nmid a_n$, o que contradiz a hipótese 1.

Não podendo ocorrer nem 1 nem 2 é porque deve ocorrer 3. Suponha-se então que 3 se verifica. Então $\alpha \nmid c_0$ e $\alpha \nmid a_1$ e $a_1 = b_0 c_1 + b_1 c_0$ o que implica $\alpha \nmid b_0 c_1$. Mas como $\alpha \nmid b_0$ e α é primo, terá de se concluir que $\alpha \nmid c_1$. Mas então $\alpha \nmid c_0$ e $\alpha \nmid c_1$ e $\alpha \nmid a_2$ e $a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0$ o que implica $\alpha \nmid b_0 c_2$. Como $\alpha \nmid b_0$ e α é primo, terá de se concluir que $\alpha \nmid c_2$. Continuando um raciocínio análogo, concluimos que $\alpha \nmid c_k$ com $k=0, \dots, s$. Por último e atendendo a que $a_n = b_r c_s$ e $\alpha \nmid c_s$, tem-se que $\alpha \nmid a_n$ o que é absurdo. O absurdo resultou de se ter suposto que p não era irredutível. Logo p é irredutível, c.q.d. ♣⁶

Vejamos outro exemplo.

Estude-se a irredutibilidade de $x^4 + x^3 + x^2 + x + 1$ sobre $\mathbb{Q}[X]$. Será que, mediante algum artifício poderemos aplicar o teorema de Eisenstein a este polinómio? Faça-se a substituição se x por $x+1$.

$$f(x+1) = (x+1)^4 + (x+1)^3 + (x+1)^2 + (x+1) + 1$$

⁶ O teorema 11 é apenas um critério e que nem sempre permite determinar polinómios irredutíveis de $\mathbb{Q}[X]$. Por exemplo, x^2+3 não verifica as condições do teorema e contudo é irredutível sobre os racionais.

$$f(x+1) = x^4 - 5x^3 + 10x^2 + 10x + 5$$

Podemos agora aplicar o teorema, com o primo 5 e concluir que $f(x+1)$ é irredutível. Mas então $f(x)$ também é irredutível uma vez que, fazendo $y=x+1$ concluimos ser $f(y)$ irredutível.

Provemos um último teorema.

Teorema 12

Seja f um polinómio tal que $f = a_0 + a_1x + \dots + a_nx^n, a_n \neq 0$. Se $\frac{r}{s}$ for uma raiz racional de f (com $r \in \mathbb{Z}$ e $s \in \mathbb{Z} \setminus \{0\}$ e r e s primos entre si), então $r \mid a_0$ e $s \mid a_n$.

Demonstração:

Se $\frac{r}{s}$ é raiz de $f(x)$ então $f(\frac{r}{s}) = 0$; ou seja

$$a_0 + a_1(r/s) + \dots + a_{n-1}(r/s)^{n-1} + a_n(r/s)^n = 0$$

Desembaraçando de denominadores, vem

$$s^n a_0 + a_1 s^{n-1} r + \dots + a_{n-1} r^{n-1} s + a_n r^n = 0$$

e logo

$$r(a_1 s^{n-1} + \dots + a_{n-1} r^{n-2} s + a_n r^{n-1}) = -a_0 s^n$$

Mas então o primeiro membro da equação é múltiplo de r , pelo que também o segundo membro o é. Ou seja, $r \mid a_0 s^n$. Como, por hipótese, r e s são primos entre si e s^n tem um número finito de divisores resulta que, ao fim de um número finito de tentativas, encontramos que $r \mid a_0$.

De modo análogo, se tivéssemos dado à expressão

$$s^n a_0 + a_1 s^{n-1} r + \dots + a_{n-1} r^{n-1} s + a_n r^n = 0$$

a forma equivalente

$$s(a_0 s^{n-1} + \dots + a_{n-1} r^{n-2} s) = -a_n r^n$$

e efectuando um raciocínio análogo, concluiríamos que $s \mid a_n$, como pretendíamos. ♣

Exemplo:

Estude-se a irreducibilidade de x^3-3x-1 em \mathbb{Q} . Começamos então por construir todas as possíveis fracções do tipo $\frac{r}{s}$ onde $r \nmid a_0$ e $s \nmid a_n$.

Ora, os únicos divisores inteiros de a_n e a_0 são 1 e -1. As possíveis fracções são apenas $1/1$, $-1/1$, $1/-1$, $-1/-1$; ou seja, o polinómio só pode ter duas raízes racionais, 1 e -1. Efectuando os cálculos, verificamos que $f(1) \neq 0$ e $f(-1) \neq 0$, pelo que nem 1 nem -1 são raízes. Logo x^3-3x-1 não tem raízes racionais pelo que é irreducível.

À laia de observação final, diga-se que nem sempre é tarefa fácil decidir se um dado polinómio é ou não irreducível, apesar de existirem certas regras gerais.

BIBLIOGRAFIA

- GODEMENT, R. (1966) *Cours d'Algèbre*. Hermann, Paris.
SANTOS, V. , (1994) Apontamentos de Álgebra, Universidade de Aveiro.
(1994).Apontamentos de Álgebra, Mestrado da Universidade de Coimbra